Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 29 May 2003

Current Nationwide Threat Level is

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports a Texas man faces multiple charges after slipping through security, getting onto an airplane unnoticed, and being found asleep in a parked American Eagle plane in Pennsylvania over the weekend. (See item 5)
- WUSA−News reports Maryland officials, increasing their surveillance of various pet food products that could contain Bovine Spongiform Encephaly, also known as mad cow disease, found 4,000 pounds of banned material that could contain the disease in Howard County. (See item 9)
- Microsoft has released "Security Bulletin MS03−018: Cumulative Patch for Internet Information Service (Important)" and a patch is available at the Microsoft website. (See item 16)
- Microsoft released "Security Bulletin MS03−019: Flaw in ISAPI Extension for Windows Media Services (Moderate)," and a patch is available at the Microsoft website. (See item 18)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: High, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *May 28, Platts Global Energy News* — **NGSA sees 'upward pressure' on summer U.S. gas prices. U.S. natural gas prices are expected to continue at or above their current levels "throughout the summer season and reach their peak when the weather is the hottest,"** the Natural Gas Supply Association (NGSA) said Wednesday its first annual summer gas

market outlook. The report was short on specific projections, however, saying instead that the domestic supply/demand scenario has become difficult to predict. NGSA said the biggest factor affecting prices −− weather −− is the most difficult to auger. **The organization, which represents many U.S. gas producers, noted that the National Oceanographic and Atmospheric Administration is predicting above−normal temperatures this summer "and will put an upward price pressure on natural gas as a result."** NGSA Chairman Bill Transier said that "while no one can accurately predict the price of natural gas in a competitive wellhead market, NGSA expects upward pressure on prices this summer. While the natural gas resource base exists, ongoing constraints burden its extraction."
Source: http://www.platts.com/stories/gas2.html

2. *May 27, The Sun, Lowell, MA* — **Massachusetts Electric wraps up $18 million equipment upgrade.** Summer is coming, and that means an increase in demand for power. And Massachusetts Electric vows to be ready. **The company says it is nearing completion on an $18 million upgrade of lines and equipment across the Merrimack Valley.** Mass Electric, a unit of British−based National Grid Transco plc, has added two new substations in Westford and North Andover, and made improvements to two others in Dracut, Billerica and Andover, according to Vice President William T. Sherry. **The company is also upgrading 20 miles of power lines and replacing 500 transformers,** he said. Sherry said Mass Electric is making upgrades in its New England and New York service areas "all the time," but added that this particular effort is "pretty precedent−setting." **Improvements are needed due to the residential and commercial growth in many communities, which led to a sharp increase in demand for electricity,** he said. Sheery said the area's summer peak demand, which in recent years has increased at about eight percent a year, forced Mass Electric to move up construction of this project. But he expects all work to be completed by next month.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3873590

3. *May 27, Platts Global Energy News* — **American firms win $466−million DOE contract for Russian work.** Washington Group International (WGI) and Raytheon were awarded a $466−million Department of Energy (DOE) contract to provide replacement power facilities as part of the department's effort to shut down three plutonium production reactors in Russia, DOE announced today. **Two of the reactors are at Seversk and one is at Zheleznogorsk. WGI is to oversee the work at Seversk, which involves refurbishing an existing fossil plant. At Zheleznogorsk, Raytheon Technical Services is to oversee the construction of a new fossil fuel plant.** At both sites, the Russian contracting firm Rosatomstroi is to serve as the integrating contractor for the Russian subcontractors. At a press conference today, DOE officials said Russians would do most of the design and construction work. However, the officials declined to provide a breakdown of the contract between the Russian and American firms, or between the two sites.
Source: http://www.platts.com/stories/nuclear1.html

4. *May 27, Albuquerque Journal* — **Honors for New Mexico wind farm.** A wind farm under construction in eastern New Mexico has already generated an award for Public Service Company of New Mexico. **The American Wind Energy Association (AWEA) this week gave PNM its Utility Leadership Award for its role in the New Mexico Wind Energy Center.** The center is a 136−turbine wind farm northeast of Fort Sumner **that will be capable of producing 204 megawatts of electricity, or enough to power about 94,000 homes.** FPL

Energy is building the farm under contract to provide the power to PNM. AWEA hands out the award each year to an electric utility that has contributed to the advancement of wind energy. **Once operational, it will be the third largest wind farm in the world, according to AWEA.** Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=bhsuper_2003_05_24_ALBJ_0000−1802−KEYWORD.Mi ssinga>

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

5. *May 28, Associated Press* — **San Antonio man accused of sneaking onto plane. A Central Texas man faces multiple charges after being found asleep in a parked American Eagle plane over the weekend in Pennsylvania. Louis Esquivel remained at the Allegheny County (PA) jail in lieu of $25,000 bond,** Police Chief Ken Fulton said. Flight attendants said they found Esquivel, 23, of San Antonio covered with a blanket in a seat in the seventh row of the plane at 5:30 a.m. Saturday. He had neither proper passenger credentials nor an airport pass, according to the arrest warrant. Esquivel told a flight attendant he was a passenger from the evening flight and simply spent the night on the plane, police said. But later, police say, he told detectives he wanted to fly the plane to St. Louis. "I mean literally fly it," Fulton said. **Police were concerned how someone could slip through security and get onto an airplane unnoticed. Detectives reviewed video surveillance that showed Esquivel enter a baggage conveyor area under repair. From there, he went through a tunnel, got on the Tarmac, and jumped aboard a United Airlines van where he found the keys in the ashtray, according to the affidavit. He drove to a gate and boarded the plane, where he was found,** officials said. Esquivel has paranoid schizophrenia, according to a San Antonio police missing−person report.
   Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/192756 9

6. *May 27, Associated Press* — **Mexico plans to X−ray all vehicles at borders. Mexico is developing a vehicle X−ray system it plans to install at crossings along its northern and**

southern borders in order to better catch would−be terrorists as well as drug and people smugglers, Foreign Secretary Luis Ernesto Derbez said Monday. Derbez said that **by the end of the year, the government hopes to equip commercial and passenger border crossings with Guatemala and Belize to the south and the United States to the north with enough X−ray machines to scan every vehicle entering the country.** Derbez said Mexico's top priorities remain the Americas' war on terrorism and promoting some form of migration agreement with Washington to better−protect undocumented Mexicans living and working in the United States.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/front/1926266

7. *April 30, Government Accounting Office* — **Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk−Based Plan Needed.** The Government Accounting Office published GAO−03−435 on April 30 concerning the topic of Rail Safety and Security. The Government Accounting Office was asked to examine recent steps taken by industry and government to improve the safety and security of hazardous materials shipped yearly across the U.S. **Serious incidents involving these materials have the potential to cause widespread disruption of injury. The GAO recommends the Secretary of Homeland Security work with the Secretary of Transportation to develop a risk−based plan to specifically address rail security.** The plan should establish time frames for actions to protect hazardous material rail shipments.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−03−435

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

8. *May 28, Wisconsin Ag Connection* — **Canada investigates how restricted feed was used. Canadian officials are talking to 200 farmers who may have received pig and poultry feed made from the rendered remains of a cow that had Bovine Spongiform Encephaly (BSE), or mad cow disease, the country's chief veterinarian said on Monday.** "We are doing a blitz investigation on 200 additional farms, just verifying the level of compliance in Canada with all the feed−related measures," Brian Evans of the Canadian Food Inspection Agency told reporters. **The cow's carcass did not go into the human food supply, but was sent to a rendering plant, which turned it into animal protein and sold it to 10 feed mills.** Since 1997, such protein has been banned from cattle feed because it is thought infected feed can cause BSE in cattle that eat it. **Evans said officials do not suspect the 200 farmers of misusing the feed, but want to make sure it was labeled, mixed and used properly.**
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=5 90t>

9. *May 28, WUSA−News* — **Feed linked to mad cow case found in Maryland.** As Maryland officials increased their surveillance of various pet food products that could contain Bovine

Spongiform Encephaly−−also known as mad cow disease−−they found banned material that could contain the disease in Howard County. **"I found 4,000 pounds of the material," says Maryland State chemist Warren Bontoyan. " We issued a stop sale (order) and made it known that they are not to remove this material under penalty of law." The specific grain is linked to North America's first case of mad cow, and is believed to be the same fed to a cow in Alberta, Canada who came down with the disease. The seized pet food comes from Pantry Pet International Products.** The U.S. ban did not address stockpiles that may be on store shelves already. **Maryland officials however did chase down those supplies, by seeking out that lot Wednesday, and removing the samples that were found in Howard County.** "The pet food that was being looked for was found. Whether it has been tested and is contaminated, that's what we still need to know," said Dr. Ivan Walks, a former DC public health director.
Source: http://www.wusatv9.com/news/news_article.asp?storyid=18786

[Return to top]

Food Sector

10. *May 28, Food and Drug Administration* — **FDA announces steps to streamline collection of information on food imports. The U.S. Food and Drug Administration (FDA) and the Bureau of Customs and Border Protection (CBP) announced today that they will streamline the implementation of the prior notice requirements of the Bioterrorism Act by allowing food importers to provide required information on food imports to both agencies using an integrated process.** Under the Act, importers will soon be required to provide "prior notice" about the content of their food imports to FDA, starting no later than December 12, 2003. Since the Act was passed last year, FDA and CBP have worked together to find ways to modify CBP's Automated Commercial System, currently used to obtain import information required by Customs. As a result of this collaboration, importers, in most circumstances, will be able to provide the required information to FDA using this existing system, making it easier for them to comply with the new law.
Source: http://www.fda.gov/bbs/topics/NEWS/2003/NEW00911.html

11. *May 28, Iowa Ag Connection* — **Bill introduced to protect consumers from unsafe meat.** Senator Tom Harkin Wednesday introduced legislation to protect consumers from pathogens in meat and poultry. **The Meat and Poultry Pathogen Reduction Act of 2003, known as "Kevin's Law," would give the U.S. Department of Agriculture (USDA) the authority to enforce food safety and sanitation standards that have been under serious attack in the federal courts.** In 1996, USDA adopted new rules to help them enforce basic safety and sanitation standards in the production of meat and poultry. These rules, called Pathogen Reduction and Hazard Analysis Critical Control Points (HACCP), are critical to ensuring that pathogens and disease are kept out of meat and poultry in restaurants and on grocery store shelves. The courts struck down USDA's ability to enforce pathogen standards for Salmonella and to require meat grinders to stop using low−quality, potentially contaminated beef trimmings. A later law suit now threatens USDA's ability to shut down a plant that repeatedly violates basic sanitation regulations. **Kevin's Law gives USDA the authority to enforce existing standards for pathogens such as Salmonella and E.Coli. It requires USDA to set standards for the food−borne pathogens based upon the best available science and**

reasonably available technology to reduce contamination.
Source: http://www.iowaagconnection.com/story−state.cfm?Id=41203

[Return to top]

Water Sector

12. *May 27, Rocky Mountain News* — **$900 million water pipeline in the works for Colorado. Colorado Springs, CO plans to build a 45−mile, $900 million water pipeline, the first in a wave of large water projects that thirsty cities are proposing across the state.** The still−unnamed pipeline will draw water from the Arkansas River below Pueblo Reservoir and deliver it north to the city by 2007. **When completed, the pipeline will expand Colorado Springs' water supplies by 75 percent, delivering enough to serve up to 900,000 people by 2040, more than twice the city's current size, according to Colorado Springs Utilities.** Large enough for the average fourth−grader to walk through, the pipeline will eventually deliver 68 million gallons of water a day to Colorado Springs and 10 million gallons a day to Fountain. In addition to the pipeline, the project also will include two new reservoirs in El Paso County and several pump stations.
Source: http://www.rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_1991736,00.html

13. *May 22, Environmental Protection Agency* — **EPA awards water security training grants. As part of U.S.Environmental Protection Agency's (EPA) initiative to help small drinking water utilities assess their vulnerabilities to terrorism, EPA Assistant Administrator for Water G. Tracy Mehan III announced the awarding of $1.5 million in grants for Water Security Training and Assistance to five nonprofit training and technical assistance organizations.** The program is authorized under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.
Source: http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/0b6f7c86157add6b85256d2e0070e96d?OpenDocument

[Return to top]

Public Health Sector

14. *May 28, Associated Press* — **SARS shuts Toronto school, 6,400 in quarantine. Concern about Severe Acute Respiratory Syndrome (SARS) shut down a Toronto, Canada area high school on Wednesday, sending staff and students into quarantine and raising fears the virus may have spread from hospitals to the broader community. More than 6,400 people, including 2,000 from the school, are now in quarantine in greater Toronto after SARS resurfaced six days ago. Health officials said a student at the school, located just north of Toronto, appeared to have symptoms of SARS, and that prompted the quarantine call.** One of the student's parents worked at Toronto's North York General Hospital, epicenter of the latest outbreak. "The risk of getting SARS in this kind of setting (a school) is very low," said Dr. Murray McQuigge, a physician in the region where the high school is located. "We are not aware of any other student in this school who is symptomatic

right now."
Source: http://www.washingtonpost.com/wp−dyn/articles/A49008−2003May 28.html

15. *May 28, New York Times* — **WHO expected to gain broader powers.** The World Health Organization's (WHO) 192 member nations are expected today to grant it sweeping new powers to respond to international health threats like Severe Acute Respiratory Syndrome (SARS) and bioterrorist attacks. **Under the resolution, to be adopted today at the organization's annual meeting in Geneva, the WHO would gain the power to set up an instant communication network, tap unofficial but reliable sources of information, and send its own teams to see if countries are doing enough to control outbreaks that could threaten other countries.** The broad new powers were approved yesterday by a policy−making committee of the United Nations agency. Member countries routinely ratify committee decisions, said Iain Simpson, a spokesman for the WHO. Simpson acknowledged that "like most instruments of international law, the resolution does not have legal teeth." Still, he said: "Any country has an ultimate veto over allowing a visitor entry; there's no way around that. But it gives us a lot of leverage."
Source: http://www.nytimes.com/2003/05/28/science/sciencespecial/28I NFE.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

16. *May 29, Microsoft* — **Microsoft Security Bulletin MS03−018: Cumulative Patch for Internet Information Service. This patch supercedes all previous patches released for IIS 4.0 and IIS 5.0. It also fixes the following vulnerabilities affecting IIS 4.0, 5.0 and 5.1**: a Cross−Site Scripting (CSS) vulnerability affecting IIS 4.0, 5.0 and 5.1 involving the error message that's returned to advise that a requested URL has been redirected; a buffer overrun that results because IIS 5.0 does not correctly validate requests for server side includes; a denial of service vulnerability that results because of a flaw in the way IIS 4.0 and 5.0 allocate memory requests when constructing headers to be returned to a web client; a denial of service vulnerability that results because IIS 5.0 and 5.1 do not correctly handle an error condition when an overly long WebDAV request is passed to them. **This patch, rated "Important," requires the patch from Microsoft Security Bulletin MS02−050 to be installed.**
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−018.asp

17. *May 28, Washington Post* — **FCC urged to release airwaves for public−safety use. A division of Northrop Grumman Corp. said Tuesday that it is petitioning the Federal Communications Commission (FCC) to reallocate 10 megahertz of spectrum in the 700−megahertz frequency range so that the Department of Homeland Security and public−safety agencies can set up advanced wireless communications systems**. Northrop is hoping to eventually profit from the federal government's increasing need for a more sophisticated, faster way to coordinate the communications between various branches of the government. The spectrum in question is now used by television broadcasters, although they are expected to abandon it when they adopt newer digital technology. **Eventually, most of the spectrum in the 700 megahertz range will be vacated and auctioned off; Northrop wants the additional spectrum to go to the government without getting auctioned off to commercial service providers**.
Source: http://www.washingtonpost.com/wp−dyn/articles/A46287−2003May 27.html?referrer=email

18. *May 28, Microsoft* — **Microsoft Security Bulletin MS03−019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service.** When Windows Media Services are installed in Windows NT 4.0 Server or added through add/remove programs to Windows 2000, nsiislog.dll is installed to the Internet Information Services (IIS) Scripts directory on the server. **A flaw in the way in which nsiislog.dll processes incoming requests could allow and attacker could send specially formed communications to the server that could cause IIS to stop responding to Internet requests**. An attacker attempting to exploit this vulnerability would have to be aware which computers on the network had Windows Media Services installed on it and send a specific request to that server. **Microsoft has assigned a risk rating of "Moderate" to this vulnerability and a patch is available at the Microsoft website.**
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−019.asp

19. *May 27, Associated Press* — **Microsoft pulls XP update over glitch. Microsoft withdrew a security update for its Windows XP software Tuesday after it crippled Internet connections for some of the 600,000 users** who had installed it since its release Friday. Consumers could reconnect only by removing the update. Microsoft officials said **the update apparently was incompatible with popular security software from other companies**. The glitch occurs amid a debate in Washington among cybersecurity experts about whether the technology industry should test the reliability and security of such updates more aggressively. **Hackers can easily attack government systems where updates aren't installed routinely, but some experts install them only reluctantly because of worries about unintended consequences of some updates**. Microsoft was still investigating the glitch and could not say when the update might be available again.
Source: http://www.washingtonpost.com/wp−dyn/articles/A45119−2003May 27.html

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **PE_FUNLOVE.4099** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	445 (microsoft−ds), 137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 139 (netbios−ssn), 113 (ident), 0 (−−−), 4899 (radmin), 17300 (Kuang2TheVirus), 4662 (eDonkey2000) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

20. *May 28, New York Times* — **Saudis arrest at least eight men believed tied to bombings.** A series of police raids around the holy city of Medina have led to the capture of up to eight suspected militants wanted in the bombing attacks against residential compounds in the Saudi capital, including the possible mastermind and perhaps two of the clerics who backed the attacks with religious sanction. **The Saudi interior minister, Prince Nayef bin Abdel Aziz, confirmed that a number of arrests had been made late Tuesday and in previous days. But he provided few details in his statement to the official Saudi Press Agency, noting only that the investigation is continuing.** Western diplomats and Saudi newspaper reports said at least three and perhaps as many as eight men had been arrested who were linked to the May 12 bomb attacks that left 25 people dead, along with nine suicide bombers. Saudi and American officials say that al Qaeda, the terrorist network founded by the Saudi−born Osama bin Laden, remains the prime suspect in the attack.
Source: http://www.nytimes.com/2003/05/28/international/middleeast/2 8CND−SAUD.html

21. *May 28, Associated Press* — **Bali suspect admits ties to terror group.** A key Bali bombing suspect admitted in court Wednesday that he was the operational chief of the Southeast Asian terror group Jemaah Islamiyah, and said he knows Osama bin Laden "very well." **Ali Ghufron, alias Mukhlas, testified at the treason trial of Abu Bakar Bashir, a Muslim cleric and the alleged spiritual head of Jemaah Islamiyah. Mukhlas told a packed courtroom he took over as the operations chief after his predecessor, Riduan Isamuddin, alias Hambali, went into hiding.** Mukhlas was arrested last year for allegedly masterminding the Oct. 12 Bali bombings, which killed 202 people. He is facing trial on terror charges for the attack, the deadliest since September 11, 2001.
Source: http://www.washingtonpost.com/wp−dyn/articles/A48406−2003May 28.html

22.

May 27, Ascribe Newswire — **National homeland security consortium, web site established by Ohio State University.** A consortium led by Ohio State University of more than 50 major universities and a host of smaller institutions has created a clearinghouse to collect, store and disseminate that kind of information. The National Academic Consortium for Homeland Security is the brainchild of Dr. Todd Stewart, retired Air Force major general and executive director of Ohio State's Program for International and Homeland Security. **Stewart knew that much of the nation's knowledge concerning research and education on security and terrorism issues was housed in the minds of the country's university scholars and scientists. He wanted to produce a quick and painless way that people could tap that knowledge base. And the World Wide Web provided a perfect vehicle for that.** His Web site (http://www.osu.edu/homelandsecurity/) provides users with a quick and effective doorway to mountains of information about ongoing programs. Users can run searches based on four specific categories − focus area, program type, university and/or state.
Source: http://www.ascribe.org/cgi−bin/spew4th.pl?ascribeid=20030523 .115318t>

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or